PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A1

(11) International Publication Number: **WO 99/47989**

(43) International Publication Date: 23 September 1999 (23.09.99)

(21) International Application Number: PCT/US99/05218

(22) International Filing Date: 10 March 1999 (10.03.99)

(30) Priority Data:
09/040,649 17 March 1998 (17.03.98) US

(71) Applicant: VERIDICOM, INC. [US/US]; 2338 Walsh Avenue, Santa Clara, CA 95051 (US).

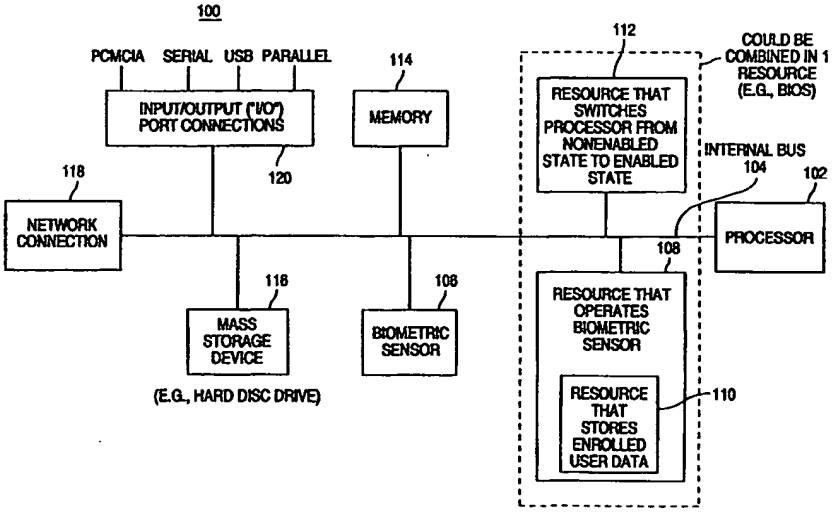
(72) Inventors: DEWELL, Sherod, E., Jr.; 4307 Woodmere Road, Tampa, FL 33609 (US). RUSSO, Anthony, P.; 206 Bellevue Avenue #2, Upper Montclair, NJ 07940 (US). O'GORMAN, Lawrence; 18 Albright Circle, Madison, NJ 07940 (US). DERBY, Robert, T.; 208 S. Park Street, San Angelo, TX 76901 (US). CHENG, Ericson, W.; Apartment 40, 1571 W. El Camino Real, Mountain View, CA 94040 (US). FITZGERALD, James, D.; 26025 Highland Way, Los Gatos, CA 95053 (US).

(74) Agents: LO, Elaine, H. et al.; Skjerven, Morrill, MacPherson, Franklin & Friel LLP, Suite 700, 25 Metro Drive, San Jose, CA 95110 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: INTEGRATED BIOMETRIC AUTHENTICATION FOR ACCESS TO COMPUTERS



(57) Abstract

The present invention is a system and a method for the use of a biometric feature as a key to grant access to a computer. The computer comprises a processor connected to a biometric sensor and a resource for operating the biometric sensor. The processor has a nonenabled state and an enabled state. In the nonenabled state the processor cannot execute applications loaded into memory from a hard drive. In the enabled state the processor can execute such applications. A user gains access to the computer and enables the processor by having a biometric feature input onto the computer using the biometric sensor. The resource that operates the biometric sensor then compares data representing the biometric feature to enrolled user data contained within the resource. If the data representing the biometric feature matches the enrolled user data then the resource switches the processor from the nonenabled state to the enabled state. If there is not a match then the processor remains in the nonenabled state.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTEGRATED BIOMETRIC AUTHENTICATION FOR ACCESS TO COMPUTERS

Related Art

The invention relates to a system and method for the use of biometric features to control access to a system, and more particularly to a system and method for the use of biometric features to control access to a computer.

Background of the Invention

Controlling access to information and especially information stored on computers is a problem that people and organizations must confront on a daily basis. A variety of systems and methods are currently used to protect information and computers from unauthorized access or interference. The most common protection systems and methods include the use of a password which must be supplied by a user.

A password based protection system or method depends on a piece of critical information, the password, for access to be gained to the information or computer. As long as the password is retained by the rightful user, access by others will be deterred. However, if the password is secured from the rightful owner whether by theft, fraud, duress, surveillance, or consent, someone other than the rightful user could obtain access to the information or computer. Additionally, for password based systems and methods longer passwords are harder for unauthorized users to guess, but they are also harder for authorized users to remember.

Furthermore, in some password based protection systems or methods the password or the program implementing the password protection is stored on a mass storage device such as a hard disk drive in the computer. These password protection systems and methods can be circumvented by replacing the mass storage device with another one, inserting a computer program on the mass storage device

which when executed will inhibit operation of the password protection programming or which will allow access to the computer or the sensitive information stored on the computer.

Therefore what is needed is a protection system and method which is based on critical information that is easily accessible to the authorized user, hard to steal, forge, or fabricate and which prevents the computer from executing programs or applications stored on a mass storage device connected to the computer

Summary of the Invention

In one embodiment of the present invention a biometric feature of a user's body serves as a key to grant access to a computer. In this embodiment the computer includes a biometric sensor, a processor, the processor being coupled to the biometric sensor, and a resource for operating the biometric sensor, the resource being coupled to the biometric sensor.

The processor has an enabled state and a nonenabled state. In the enabled state, the processor has loaded an operating system into a memory coupled to the processor so that the processor can execute computer programs loaded into memory from a mass storage device such as a hard disk drive, a CD ROM or computer programs loaded from a source external to the computer such as the Internet. In the nonenabled state, the processor cannot execute commands as part of a computer program loaded into memory from a mass storage device or from an source external to the computer.

The resource for operating the biometric sensor is initiated by a user input. A suitable user input includes the user operating a power switch to turn on the computer. In response to the user input, the resource operates the biometric sensor. The biometric sensor reads biometric information from the biometric sensor, the biometric information being input into the sensor as part of the user input. Any biometric information will suffice, including but not limited to a retinal image, a palm print, a signature, facial features, or a fingerprint. In the case where a fingerprint is used, the biometric information read from the biometric sensor includes information representing a fingerprint. For a valid user input, which in

the present embodiment includes information representing a user fingerprint which corresponds to information representing a valid fingerprint stored in the computer, the resource changes the processor from the nonenabled state to the enabled state. In one embodiment of the invention the resource includes a basic input and output system (a "BIOS" program). A BIOS program in a traditional personal computer is a program stored in the computer in a nonvolatile memory, the BIOS memory, which typically begins operation once the computer is powered on and completes its operation by loading an operating system. In this embodiment, after the resource verifies that the user input includes a valid user input, the BIOS program is allowed to finish its operation and loads an operating system, enabling the processor to run computer applications or computer programs. In the present embodiment if the user input does not include a valid user input then the resource, the BIOS program in this embodiment, will not allow the computer to load an operating system. The processor thus remains in the nonenabled state and can not run computer programs stored on a mass storage device couple to the computer, and the computer cannot access information stored within the computer.

Another embodiment of the present invention is a computer for integrated biometric access control comprising a processor, a biometric sensor coupled to the processor, a resource coupled to the biometric sensor that operates the biometric sensor, and a resource coupled to the processor that switches the processor from a nonenabled state to an enabled state after operation of the resource that operates the biometric sensor. In one aspect of the invention the enabled state of the processor includes an operating system loaded into a memory. In another aspect of the invention the enabled state of the processor includes loading a program from a mass storage device connected to the computer into a memory connected to the computer. In yet another aspect of the invention, the processor in the nonenabled state cannot load an operating system.

In another embodiment of the invention, the resource that operates the biometric sensor includes a resource that reads data from the biometric sensor, wherein the data represents a biometric feature. In another aspect of the invention,

the resource that operates the biometric sensor includes a resource that stores enrolled user data. In still another aspect of the invention the resource that operates the biometric sensor includes a resource that compares the data from the biometric sensor to information stored in the computer. In another aspect of the invention if the data matches the information stored in the computer within predetermined limits, then the resource that switches the processor from the nonenabled state to the enabled state is allowed to switch the processor to the enabled state. In this aspect of the invention if the data does not match the information stored in the computer, then the resource that switches the processor from the nonenabled state to the enabled state is prevented from switching the processor into the enabled state. In one embodiment, the information stored in the computer includes enrolled user data.

Still another embodiment of the invention comprises a processor, an internal bus, the internal bus being connected to the processor, and a biometric sensor, the biometric sensor being connected to the internal bus. In one aspect of the invention the biometric sensor includes a resource that reads biometric information from the biometric sensor. In another aspect of the invention the biometric sensor includes a resource that operates the biometric sensor before loading an operating system. In yet another aspect of the invention the resource that operates the biometric sensor includes a resource that stores enrolled user data. In still another aspect of the invention, the resource that reads data from the biometric sensor includes a resource that automatically determines a set of default settings for the representing the biometric feature.

In yet another aspect of the invention the resource that operates the biometric sensor includes a resource that compares the biometric information from the biometric sensor to information stored in the computer. In another aspect of the invention if the biometric information from the sensor matches the information stored in the computer within predetermined limits, then the resource that operates the biometric sensor before loading the operating system is allowed to load the operating system. In this aspect of the invention if the biometric information from

the sensor does not match the information stored in the computer, then the resource that operates the biometric sensor before loading the operating system is prevented from loading the operating system.

Yet another embodiment of the invention is a method of integrated biometric authentication for access to a computer, the method comprising reading data representing a biometric feature, and attempting to authenticate the biometric feature before loading an operating system.

Still another embodiment of the invention is a method of enrolling a user in an integrated biometric authentication system for access to a computer, the method comprising reading data representing a biometric feature and storing the data in a nonvolatile memory. In one aspect of the invention the nonvolatile memory includes a BIOS memory or a part of a BIOS memory. Yet another aspect of this embodiment of the invention comprises storing biometric authentication software in the nonvolatile memory. In still another aspect of this embodiment of the invention storing biometric authentication software in the nonvolatile memory includes storing a verification program in the nonvolatile memory.

Brief Description of the Figure

Figure 1 depicts a computer in accordance with on embodiment of the invention.

Figure 2 is a flowchart depicting the operating of one embodiment of the invention. A user's biometric information is read and compared to enrolled user data in order to determine if the user should be granted access to the computer.

Figure 3 is a flowchart depicting the enrollment of users in an embodiment of the present invention.

Figure 4A depicts a general menu of a graphical user interface of an embodiment of the enrollment software of the invention.

Figure 4B depicts a users menu of a graphical user interface of an embodiment of the enrollment software of the invention.

Figure 5 depicts a computer with a BIOS memory in accordance with on embodiment of the invention.

Figure 6 depicts a memory allocation of a BIOS memory, extension in accordance with an aspect of the invention.

Detailed Description

The following description is presented to enable a person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments disclosed, but is to be accorded the widest scope consistent with the principles and features disclosed herein.

Figure 1 depicts an embodiment of the invention. Computer 100 includes a processor. Processor 102 is any type of processor such as a microprocessor, dedicated logic, a digital signal processor, a programmable gate array, a neural network, or a central processor unit implemented in any other technology. Processor 102 is coupled to internal bus 104. Although Figure 1 depicts processor 102 being directly coupled to internal bus 104, processor 102 could be coupled to internal bus 104 through a bus controller. Internal bus 104 could be an ISA bus a micro-channel bus, a VESA bus, a PCI bus, or any other system or host bus.

Biometric sensor 106 is coupled to processor 102 through internal bus 104. Biometric sensor 106 senses a biometric feature such as fingerprints, retinas, palm prints, irises, faces, signature, or any other biometric attribute or characteristic. Although only one biometric sensor is shown in Figure 1, any number of sensors could be connected to the computer in any combination allowing biometric features from more than one portion of a single body or more than one body to be used. Biometric sensor 106 generically represents any type of sensor including a camera, a fingerprint sensor, a laser based sensor, a pressure sensor to detect a written signature, or any other type of sensor that can be used to detect a biometric feature or attribute. Examples of biometric sensors are described in U.S. Patent

Application No. 08/573,100, entitled "Fingerprint Acquisition Sensor," inventors: Alexander G. Dickinson, Ross McPherson, Sunetra Mendis and Paul C. Ross, filed 12/15/95, U.S. Patent Application No. 08/855,230 entitled "Capacitive Fingerprint Sensor with Adjustable Gain," inventors: Alexander G. Dickinson, Ross McPherson, Sunetra Mendis and Paul C. Ross, filed 5/13/97, and U.S. Patent Application No. 08/971,455 entitled "Automatic Adjustment Processing for Sensor Devices," inventors: Anthony P. Russo, and Lawrence O'Gorman, filed 11/17/97. All three applications are commonly owned with the present application and all three applications are hereby incorporated by reference.

Resource 108 operates biometric sensor 106 and is coupled to processor 102 through internal bus 104. Resource 108 includes resource 110 which stores enrolled user data. The enrolled user data represents the biometric features of users who have been granted access to computer 100. The enrolled user data could be stored in any way that can be compared to the data generated by biometric sensor 106. One example of a cryptographic storage technique that can be used is described in U.S. Patent Application No. 08/857,642 entitled "Identification and Security Using Biometric Measurements," inventors: Peter Kelley Pearson, Thomas Edward Rowley, and Jimmy Ray Upton filed 5/16/97.

Resource 112 switches processor 102 from a nonenabled state to an enabled state and is coupled to processor 102 through internal bus 104. In other embodiments of the invention, resource 110 is not included within resource 108, but is a separate resource. In still other embodiments, resources 108, 110 and 112 are all combined into one resource, and in still other embodiments biometric sensor 106 is directly coupled to resource 108. Memory 114 is coupled to processor 102 through internal bus 104. Memory 114 may includes system memory, and cache memory.

Computer 100 may also include mass storage device 116, network connection 118, and/or one or more input/output ("I/O") ports 120. In other embodiments of the invention, sensor 106 can be coupled through I/O ports 120 to internal bus 104. Mass storage device 116 may include, but is not limited to a hard

disk drive, a CD ROM drive, or a DVD Drive. Network connection 118 may includes but is not limited to an intranet connection, an internet connection, a world wide web connection, or any other connection to another computer.

In one embodiment of the invention, when processor 102 is in the nonenabled state computer programs or applications stored in memory 114, mass storage device 116 or input through network connection 118 cannot be executed by processor 102. In another embodiment of the invention the nonenabled state of the processor includes the situation in which an operating system has not been loaded into memory 114. In another embodiment of the invention, when processor 102 is in the enabled state computer programs or applications stored in memory 114, mass storage device 116 or input through network connection 118 can be executed by processor 102. For a processor in a personal computer, the enabled state of the processor includes the situation in which an operating system has been loaded into memory 114.

In one embodiment of the invention not depicted in Figure 1, resource 108, resource 110, and resource 112 can be incorporated in a BIOS program stored in a BIOS memory or in a BIOS memory. In another embodiment, one or more of resources 108, 110 and 112 can be incorporated into a memory in biometric sensor 106 and the remaining resource, if any, incorporated into a BIOS memory or a BIOS memory extension.

Figure 2 is a flowchart which depicts the operation of one embodiment of the present invention. In step 202 computer 100 is powered on, processor 102 is in the nonenabled state, and the computer then proceeds to step 204. In step 204 resource 108 operates the biometric sensor. In other embodiments of the invention, step 204 can occur at any time during the start up process of the computer from power on step 202 until the processor is switched into the enabled state. In an embodiment of the present invention in which the computer is a personal computer and resources 108, I I0, and 112 are incorporated into or called by a BIOS program, step 204 can occur at any point up until the BIOS loads the operating system.

After step 204, then step 206 is executed. In step 206 resource 108 reads data representing a biometric feature from biometric sensor 106. After step 206, step 208 is executed. In step 208 the data representing the biometric feature is read until the data is meets a preset image quality standard. Optional image enhancement features may be used at this point such as those described in the U.S. Patent Applications "Capacitive Fingerprint Sensor with Adjustable Gain," inventors: Alexander G. Dickinson, Ross McPherson, Sunetra Mendis and Paul C. Ross, filed 5/13/97, and "Automatic Adjustment Processing for Sensor Devices," inventors: Anthony P. Russo, and Lawrence O'Gorman. In other embodiments of the present invention step 208 may be skipped. Next, step 210 is executed.

In step 210 resource 108 compares the data read in from the sensor to the enrolled user data stored in resource 110. Predefined tolerances defining acceptable matches between the data read in from the biometric sensor and the enrolled user data can be established. In other embodiments of the invention step 210 includes advanced matching techniques. Advanced matching techniques may include but are not limited to image processing, geometric processing, and statistical processing. Next step 212 is executed.

In step 212 if the data read in from the sensor matches the enrolled user data, or if it is within the predefined tolerances, then step 214 is executed and resource 112 switches the processor from the nonenabled state to the enabled state. In other embodiments of the invention, step 214 includes keeping a log of users who access the computer, requiring one or more other users to also be verified before the processor is enabled, or requiring the user to provide another password which may or may not be a biometric password or include biometric information.

If the match at step 212 is not close enough then step 216 is executed. At step 216 if the predefined number of retries has not been reached then the system returns to step 206. In other embodiments of the invention, if the match at step 212 is not close enough then the user is provided with a message indicating that the sensor is retrying the process, that the sensor needs to be adjusted or cleaned, or any other message which conveys information to the user in order to aid the

identification process. If the retry limit has been reached, then step 218 is executed and the processor remains in the nonenabled state. In other embodiments of the invention if the match is not close enough at step 212 then step 218 is executed directly, and in effect the retry limit is zero retries.

Figure 3 is a flowchart depicting enrollment of users in accord with an embodiment of the present invention. In the case where there are no enrolled users, at step 302, a biometric sensor is coupled to a processor of the computer if this has not already been done. Next, at step 304 the computer is turned on. Next, at step 306 the computer boots up normally and the processor is enabled. Next, if either the enrollment or verification software is not loaded, then at step 308 the missing software is loaded into the computer. In one embodiment of the invention, the verification software is loaded into the appropriate resources. For example, the verification software that operates the biometric sensor is loaded into the resource that operates the biometric sensor. In one embodiment of the invention the enrollment software is also loaded into the resource that operates the biometric sensor, and in another embodiment of the invention, the enrollment software is loaded on to a mass storage device and is run by the computer as an application.

Next, step 310 is executed and one or more users are enrolled into the system. Figures 4A and 4B represent images of graphical user interfaces in accord with one embodiment of the present invention. In Figure 4A general dialog box 402 gives the user an array of configuration choices for the enrollment and verification system. Option 404 allows a user to enable the biometric access control system. Options 406 and 408 enable optional image and quality enhancement resources such as those described in the U.S. Patent Application entitled "Capacitive Fingerprint Sensor with Adjustable Gain," inventors: Alexander G. Dickinson, Ross McPherson, Sunetra Mendis and Paul C. Ross, filed 5/13/97, and U.S. Patent Application entitled "Automatic Adjustment Processing for Sensor Devices," inventors: Anthony P. Russo, and Lawrence O'Gorman, filed.

Option 410 allows the maximum a user to set the maximum number of users that can be enrolled into the system. Option 412 allows the maximum number of retries of the verification cycle to be set. Option 414 allows the user to set the match score that will be required in order for data representing a biometric feature to be considered a close enough match with enrolled data to allow the user access to the computer. In the embodiment depicted by the flowchart of Figure 2, this option sets the match which will be required in step 212.

Option 416 allows the user to set the resolution which will be used to represent the enrolled user data. In one embodiment, when button 418 is activated, the configuration choices depicted on the general menu options discussed above will be stored in the resource that operated the biometric sensor. Status line 420 indicates that the biometric sensor is connected to the computer and working properly.

Figure 4B depicts the graphical user interface representing the users enrollment interface 448. A user places a biometric feature on the biometric sensor and selects read button 450. The biometric feature is then read by the biometric sensor and displayed in box 452. A user can enter a user id at line 454 and a password in line 456. Box 458 can be selected to save the data representing the user, including the biometric feature and the user id and password. The user's biometric feature can be designated for use as enrolled user data by selecting add button 460.

A user's enrolled user data can be called up by entering the user's user id and password. The data will then appear in box 462. The user's enrolled data can be deleted by selecting delete box 464. In one embodiment of the invention, apply button 466 updates resource 110 of Figure 1 which stores the enrolled user data. OK button 468 also updates resource 110, and additionally closes the graphical user interface box depicted in Figure 4B. Cancel button 470 cancels the changes to the enrolled user data and closes the graphical user interface box.

In another embodiment of the invention, users are enrolled into the system at a secure site and the enrolled user data is loaded into the resource that stores the

enrolled user data. In one embodiment the resource that stores the enrolled user data is nonvolatile memory which includes a BIOS program. The nonvolatile memory including the BIOS and the enrolled user data can then be incorporated into a computer. In yet another embodiment, the resource that operates the biometric sensor can also be stored in a nonvolatile memory which contains the BIOS program.

In still another embodiment of the invention, users are enrolled into the system once access to the computer has been granted to an enrolled user. In this embodiment the graphical user interfaces represented by Figures 4A and 4B are operated one the enrolled user gains access to the computer.

Figure 5 depicts another embodiment of the invention. Computer 500 comprises central processing unit 502 coupled to bus controller 504. System memory and cache 506 is also coupled to bus controller 504. Internal bus 508 is coupled to bus controller 504. Internal bus 508 could be an ISA bus a micro-channel bus, a VESA bus, a PCI bus, or any other system or host bus.

BIOS memory 510 is coupled to internal bus 508. Figure 5 depicts BIOS memory 510 as two components, host BIOS memory 512 and BIOS memory extension 514. In other embodiments of the invention, the BIOS memory extension is eliminated and the programming stored in BIOS memory extension 514 is incorporated into host BIOS memory 512.

Biometric sensor 516 is coupled to internal bus 508. In one embodiment biometric sensor 516 includes sensor controller 518 and biometric sensor device 520. Mass storage device 522, which can include but is not limited to a hard disk drive or a floppy disk drive, is coupled to internal bus 508 through mass storage device controller 524. Other devices which may be coupled to internal bus 508 include but are not limited to display controller 526 which is coupled to display 528, keyboard and keyboard controller 530, extra memory 532, and serial and parallel ports 534.

In one embodiment of the invention, the BIOS program stored in host BIOS memory 512 contains an initial program loader, which could be a bootstrap loader,

which loads the BIOS program from the host BIOS memory into system memory when the computer is first powered on. The BIOS program then tests and initializes the devices connected to the internal bus, including but not limited to the system memory, the display, the internal bus, and the keyboard. The BIOS program then begins loading an operating system or other external software, enabling the processor to execute non-BIOS programming. At any point between the time the initial program loader loads the BIOS program into the system memory and when the processor is enabled, the BIOS program searches for a particular numerical signature in a memory location. If the signature is found then the computer code appearing after the signature is executed.

Figure 6 depicts a BIOS memory extension in accord with one embodiment of the invention. In this embodiment, the BIOS program is searching for the signature 55AA. In other embodiments the BIOS program could be searching for other numerical signatures. This signature appears at 602 at the top of the BIOS memory extension. Memory location 604 contains manufacturer and version information for biometric sensor 516. Location 606 contains configuration defaults for biometric sensor 516. These configuration defaults may include those entered using the graphical user interfaces of Figures 4A and 4B. Memory location 608 contains enrolled user data. Memory location 610 contains the programming that operates the biometric sensor and allows it to read in the data representing the biometric feature and enhance the image if required. Memory location 612 contains the programming that compares the data read in from the biometric sensor to the enrolled user data.

In another embodiment of the invention, the information and computer code depicted in Figure 6 is stored in the host BIOS memory. In yet another embodiment of the invention, the information and computer code depicted in Figure 6 and the BIOS program stored in the host BIOS are both stored in the central processing unit. In another embodiment of the invention the information and computer code depicted in Figure 6 and the BIOS program stored in the host BIOS are both stored in nonvolatile memory in the biometric sensor.

The foregoing description of embodiments of the present invention are presented for the purposes of illustration and description only. They are not intended to be exhaustive or to limit the invention to the forms disclosed. Many modifications and variations will be apparent to practitioners skilled in the art. It is intended that the scope of the invention be defined by the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A computer for integrated biometric access control, comprising:

a processor;

a biometric sensor, the biometric sensor being coupled to the processor;

a resource that operates the biometric sensor, the resource being coupled to the biometric sensor; and

a resource, coupled to the processor, that switches the processor from a nonenabled state to an enabled state after operation of the resource that operates the biometric sensor.

2. The computer of claim 1, wherein the enabled state of the processor includes an operating system loaded into a memory.

3. The computer of claim 1, wherein the enabled state of the processor includes loading a program from a mass storage device connected to the computer into a memory connected to the computer.

4. The computer of claim 1, wherein the enabled state of the processor includes loading a program from a network connected to the computer into a memory connected to the computer.

5. The computer of claim 1, wherein the processor in the nonenabled state cannot load an operating system.

6. The computer of claim 1, wherein the resource that operates the biometric sensor includes a resource that reads data from the biometric sensor, and the data represents a biometric feature.

7. The computer of claim 6, wherein the biometric feature includes a fingerprint.

8. The computer of claim 1, wherein the biometric sensor is coupled to the processor by an internal bus.

9. The computer of claim 1, wherein the resource that operates the biometric sensor includes a resource that stores enrolled user data.

10. The computer of claim 6, wherein the resource that reads data from the biometric sensor includes a resource that automatically determines a set of default settings for the data representing the biometric feature.

11. The computer of claim 6, wherein the resource that operates the biometric sensor includes a resource that attempts to compare the data from the biometric sensor to information stored in the computer.

12. The computer of claim 11, wherein the resource that attempts to compare the data from the biometric sensor to information stored in the computer includes a resource that attempts to validate a user identity.

13. The computer of claim 1, wherein the biometric sensor includes a capacitive fingerprint sensor.

14. The computer of claim 1, comprising a BIOS memory including a BIOS program wherein the BIOS memory includes the resource that operates the biometric sensor.

15. The computer of claim 14, wherein the BIOS memory includes a BIOS memory extension and the BIOS memory extension includes the resource that operates the biometric sensor.

16. A computer for integrated biometric access control, comprising:

a processor;

an internal bus, the internal bus being connected to the processor; and

a biometric sensor for controlling access to the computer, the biometric sensor being connected to the internal bus.

17. The computer of claim 16, wherein the biometric sensor includes a resource that reads biometric information from the biometric sensor.

18. The computer of claim 17, wherein the biometric information includes information representing a fingerprint.

19. The computer of claim 16, wherein the biometric sensor includes a resource that operates the biometric sensor before loading an operating system.

20. The computer of claim 19, wherein the resource that operates the biometric sensor includes a resource that stores enrolled user data.

21. The computer of claim 19, wherein the resource that operates the biometric sensor includes a resource that reads data from the biometric sensor, and the data represents a biometric feature.

22. The computer of claim 21, wherein the resource that reads data from the biometric sensor includes a resource that automatically determines a set of default settings for the data representing the biometric feature.

23. The computer of claim 19, wherein the resource that operates the biometric sensor includes a resource that attempts to compare the biometric information from the biometric sensor to information stored in the computer.

24. The computer of claim 23, wherein the resource that attempts to compare the biometric information from the biometric sensor to information stored in the computer includes a resource that attempts to validate a user identity.

25. The computer of claim 16, wherein the biometric sensor includes a capacitive fingerprint sensor.

26. The computer of claim 16, comprising a parallel port connected to the bus.

27. The computer of claim 16, comprising a BIOS memory, including a BIOS program, the BIOS memory including a resource that initiates operation of the biometric sensor.

28. A method of integrated biometric authentication for access to a computer, the method comprising:

reading data representing a biometric feature; and

attempting to authenticate the biometric feature before loading an operating system.

29. The method of claim 28, wherein loading the operating system includes reading at least a portion of the operating system from a disk.

30. The method of claim 28, wherein loading the operating system includes reading at least a portion of the operating system from a network connection.

31. The method of claim 28, wherein reading data includes automatically determining a set of default settings for the data representing the biometric feature.

32. The method of claim 28, comprising storing data representing the biometric feature in a memory in the computer.

33. The method of claim 28, comprising loading the operating system after attempting to authenticate if attempting to authenticate is successful.

34. The method of claim 28, comprising not loading the operating system after attempting to authenticate if attempting to authenticate is unsuccessful.

35. The method of claim 28, wherein attempting to authenticate includes comparing the data representing the biometric feature to enrolled user data.

36. The method of claim 28, wherein the biometric feature includes a fingerprint.

37. A method of integrated biometric authentication for access to a computer, the computer including a processor, and the processor having an enabled state and a nonenabled state, the method comprising:

reading data representing a biometric feature; and

attempting to authenticate the biometric feature before switching the processor from the nonenabled state to the enabled state.

38. The computer of claim 37, wherein the enabled state of the processor includes an operating system loaded into a memory.

39. The computer of claim 37, wherein the enabled state of the processor includes loading a program from a mass storage device connected to the computer into a memory connected to the computer.

40. The computer of claim 37, wherein the enabled state of the processor includes loading a program from a network connected to the computer into a memory connected to the computer.

41. The computer of claim 37, wherein the processor in the nonenabled state cannot load an operating system.

42. The method of claim 37, wherein reading data includes automatically determining a set of default settings for the data representing the biometric feature.

43. The method of claim 37, comprising storing data representing the biometric feature in a memory in the computer.

44. The method of claim 37, wherein the switching the processor from the nonenabled state to the enabled state after attempting to authenticate occurs if attempting to authenticate is successful.

45. The method of claim 37, comprising not switching the processor from the nonenabled state to the enabled state after attempting to authenticate occurs if attempting to authenticate is unsuccessful.

46. The method of claim 37, comprising maintaining the processor in the nonenabled state after attempting to authenticate occurs if attempting to authenticate is unsuccessful.

47. The method of claim 37, wherein attempting to authenticate includes comparing the data representing the biometric feature to enrolled user data.

48. The method of claim 37, wherein the biometric feature includes a fingerprint.

49. A method of enrolling a user in an integrated biometric authentication system for access to a computer, the method comprising:

reading data representing a biometric feature; and

storing the data in nonvolatile memory in the computer.

50. The method claim 49, comprising automatically determining a set of default settings for the data representing the biometric feature.

51. The method claim 49, wherein the nonvolatile memory includes a BIOS memory, the BIOS memory including a BIOS program.

52. The method claim 49, comprising storing biometric authentication software in the nonvolatile memory.

53. The method claim 52, wherein storing biometric authentication software in the nonvolatile memory includes storing a verification program in the nonvolatile memory.

54. The method claim 49, comprising a biometric sensor, the biometric sensor including nonvolatile memory.

55. A computer for integrated biometric access control, comprising:

a processor;

a bus controller, the bus controller being connected to the processor;

a bus, the bus being connected to the bus controller;

a BIOS memory, the BIOS memory including a BIOS program, the BIOS memory being connected to the bus;

a BIOS memory extension, the BIOS memory extension being connected to the bus; and

a biometric sensor, the biometric sensor being connected to the bus.

56. The computer of claim 55, comprising a parallel port connected to the bus.

57. The computer of claim 55, wherein the BIOS memory extension includes a resource which reads biometric information from the biometric sensor.

58. The computer of claim 56, wherein the biometric information includes information representing a fingerprint.

59. The computer of claim 55, wherein the BIOS memory extension includes a resource that operates the biometric sensor before loading an operating system.

60. The computer of claim 59 wherein the resource that operates the biometric sensor includes a resource that stores enrolled user data.

61. The computer of claim 60, wherein the resource that operates the biometric sensor includes a resource that reads data from the biometric sensor, and the data represents a biometric feature.

62. The computer of claim 61, wherein the resource that reads data from the biometric sensor includes a resource that automatically determines a set of default settings for the data representing the biometric feature.

63. The computer of claim 59, wherein the resource that operates the biometric sensor includes a resource that attempts to compare the biometric information from the biometric sensor to information stored in the BIOS memory.

64. The computer of claim 63, wherein the resource that attempts to compare the biometric information from the biometric sensor to information stored in the BIOS memory includes a resource that attempts to validate a user identity.

65. The computer of claim 55, wherein the biometric sensor includes a capacitive fingerprint sensor.

66. A computer for integrated biometric access control, comprising:

a processor;

a bus, the bus being connected to the processor;

a BIOS memory, the BIOS memory including a BIOS program, the BIOS memory being connected to the bus;

a biometric sensor for sensing a biometric feature of a user, the biometric sensor being connected to the bus; and

a means for authenticating the biometric feature of the user before loading an operating system.

67. The computer of claim 66, wherein the means for authenticating includes a means for reading biometric information from the biometric sensor.

68. The computer of claim 67, wherein the biometric information includes information representing a fingerprint.

69. The computer of claim 67, including a means for storing enrolled user data.

70. The computer of claim 66, wherein the biometric sensor includes a capacitive fingerprint sensor.

71. A computer for integrated biometric access control, comprising:

a user input, the user input having a biometric sensor;

a processor, the processor having an enabled state and a nonenabled state, and the processor being coupled to the biometric sensor; and

a BIOS memory including a BIOS program, the BIOS memory having a resource that responds to the user input and for a valid user input the processor changes from the nonenabled state to the enabled state.

72. The computer of claim 71, wherein the user input includes a power switch.

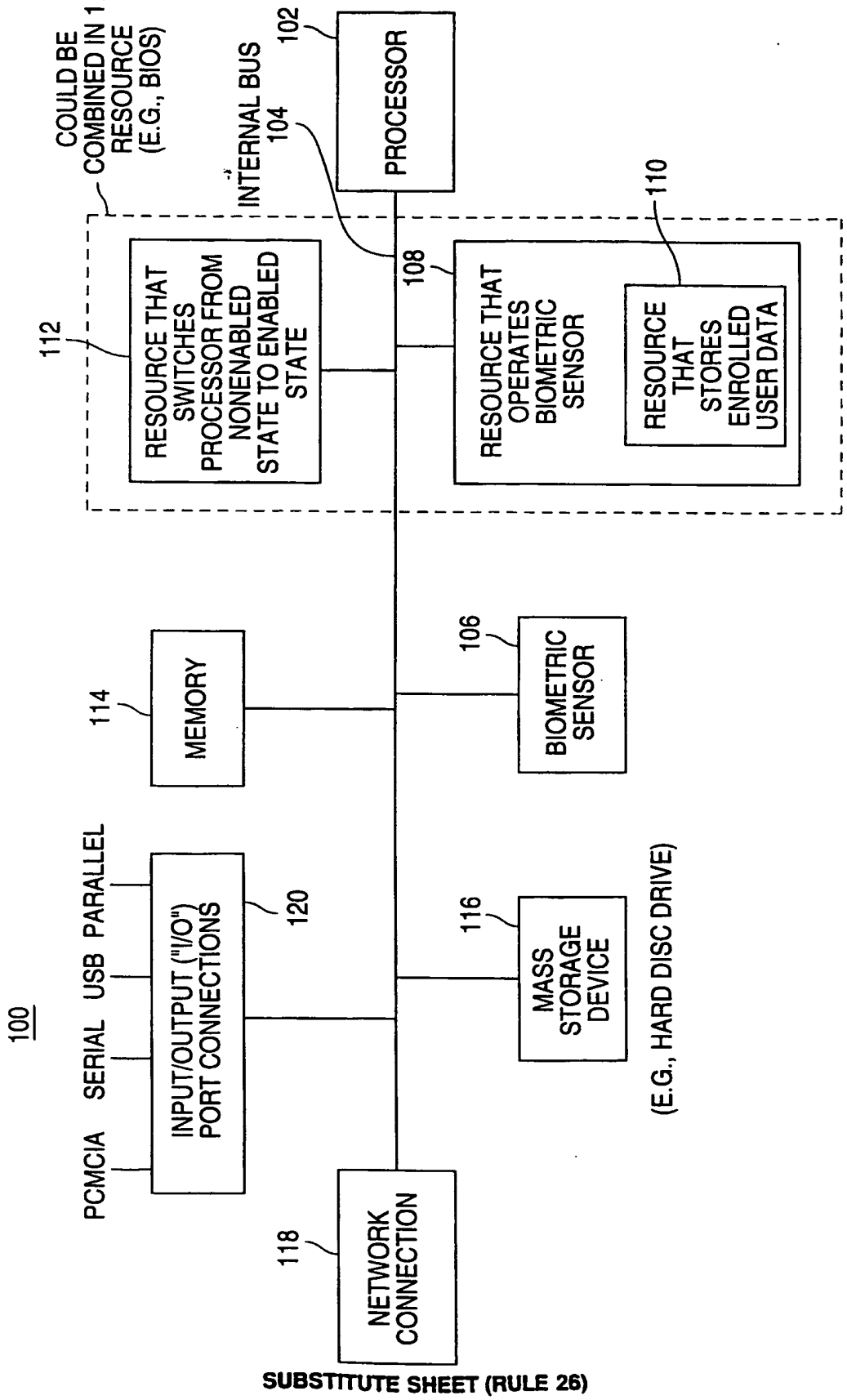

100
COULD BE COMBINED IN 1 RESOURCE (E.G., BIOS)
INTERNAL BUS 104
PROCESSOR 102
112
RESOURCE THAT SWITCHES PROCESSOR FROM NONENABLED STATE TO ENABLED STATE
108
RESOURCE THAT OPERATES BIOMETRIC SENSOR
110
RESOURCE THAT STORES ENROLLED USER DATA
MEMORY 114
BIOMETRIC SENSOR 106
PCMCIA SERIAL USB PARALLEL
INPUT/OUTPUT ("I/O") PORT CONNECTIONS 120
MASS STORAGE DEVICE 116
(E.G., HARD DISC DRIVE)
NETWORK CONNECTION 118

FIGURE 1

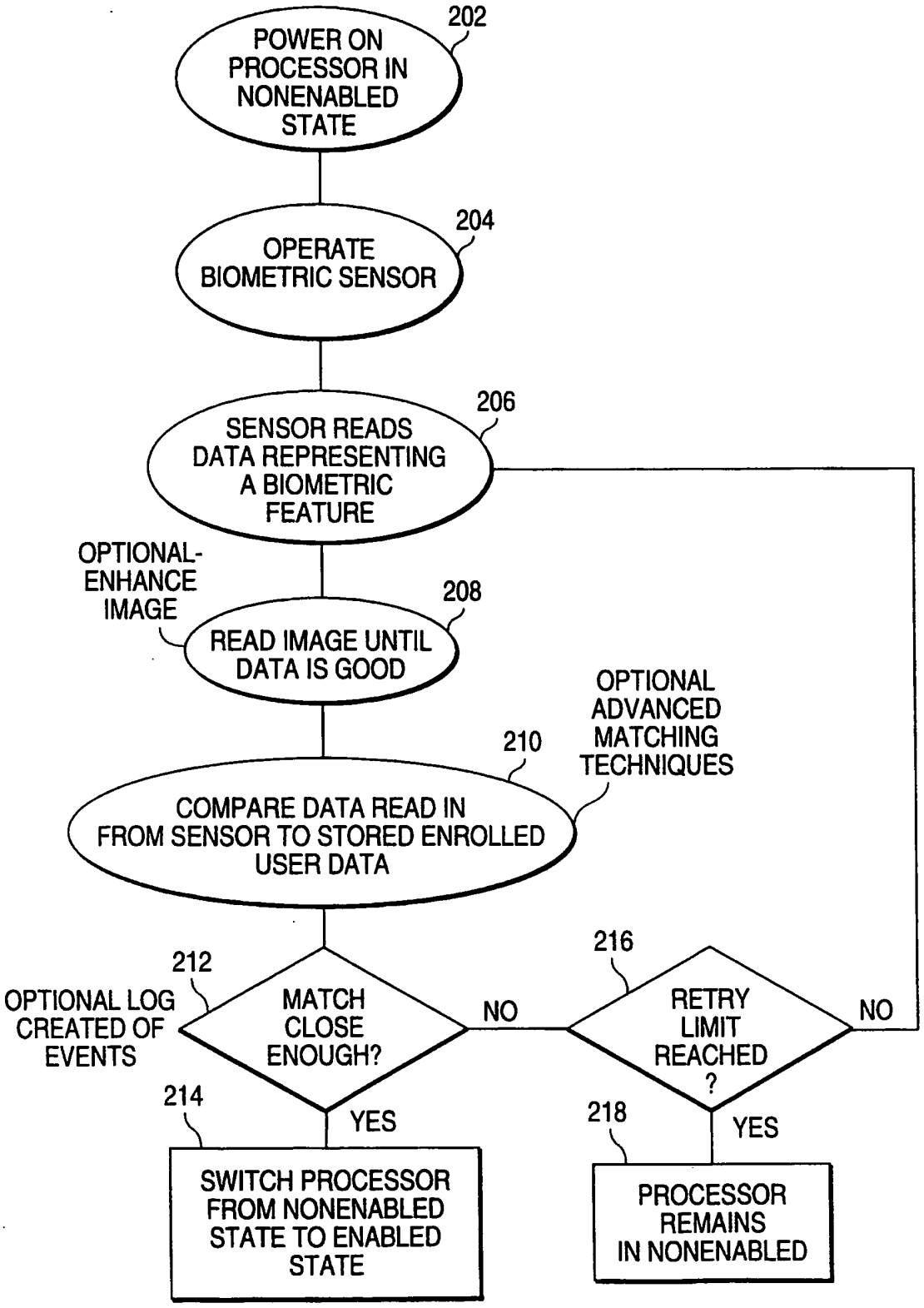

202
POWER ON PROCESSOR IN NONENABLED STATE
204
OPERATE BIOMETRIC SENSOR
206
SENSOR READS DATA REPRESENTING A BIOMETRIC FEATURE
OPTIONAL-ENHANCE IMAGE
208
READ IMAGE UNTIL DATA IS GOOD
OPTIONAL ADVANCED MATCHING TECHNIQUES
210
COMPARE DATA READ IN FROM SENSOR TO STORED ENROLLED USER DATA
212
OPTIONAL LOG CREATED OF EVENTS
MATCH CLOSE ENOUGH?
NO
216
RETRY LIMIT REACHED ?
NO
YES
214
SWITCH PROCESSOR FROM NONENABLED STATE TO ENABLED STATE
218
YES
PROCESSOR REMAINS IN NONENABLED

FIGURE 2

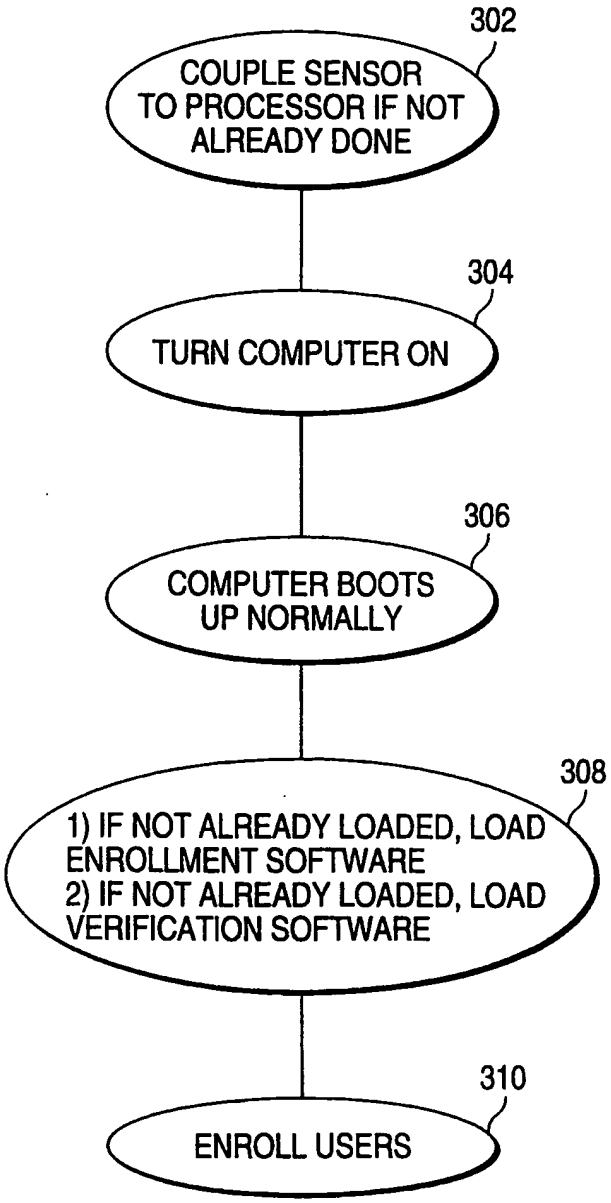

302
COUPLE SENSOR TO PROCESSOR IF NOT ALREADY DONE
304
TURN COMPUTER ON
306
COMPUTER BOOTS UP NORMALLY
308
1) IF NOT ALREADY LOADED, LOAD ENROLLMENT SOFTWARE
2) IF NOT ALREADY LOADED, LOAD VERIFICATION SOFTWARE
310
ENROLL USERS

FIGURE 3

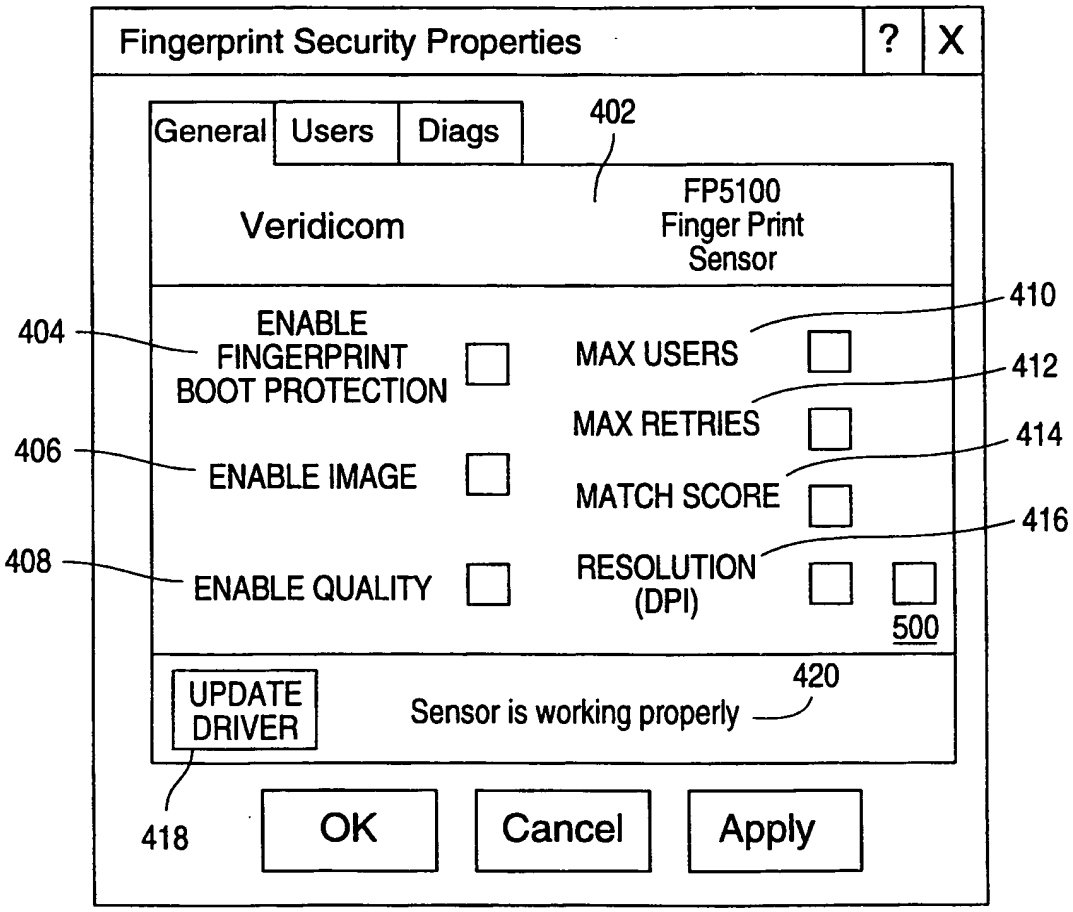

Fingerprint Security Properties
?
X
General
Users
Diags
402
Veridicom
FP5100
Finger Print
Sensor
404
ENABLE
FINGERPRINT
BOOT PROTECTION
406
ENABLE IMAGE
408
ENABLE QUALITY
410
MAX USERS
412
MAX RETRIES
414
MATCH SCORE
416
RESOLUTION
(DPI)
500
UPDATE
DRIVER
420
Sensor is working properly
418
OK
Cancel
Apply

FIGURE 4A

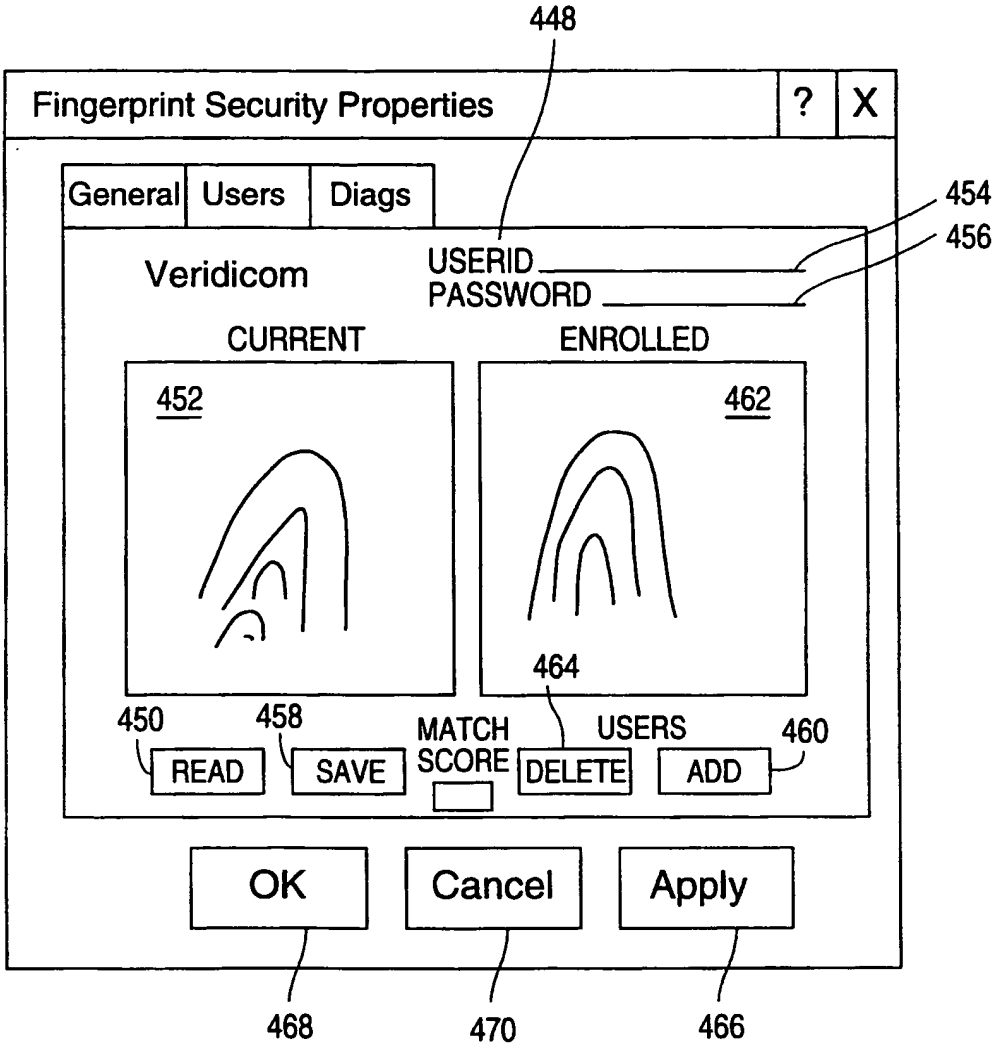

448
Fingerprint Security Properties
?
X
General
Users
Diags
454
456
Veridicom
USERID
PASSWORD
CURRENT
ENROLLED
452
462
464
450
458
MATCH SCORE
USERS
460
READ
SAVE
DELETE
ADD
OK
Cancel
Apply
468
470
466

FIGURE 4B

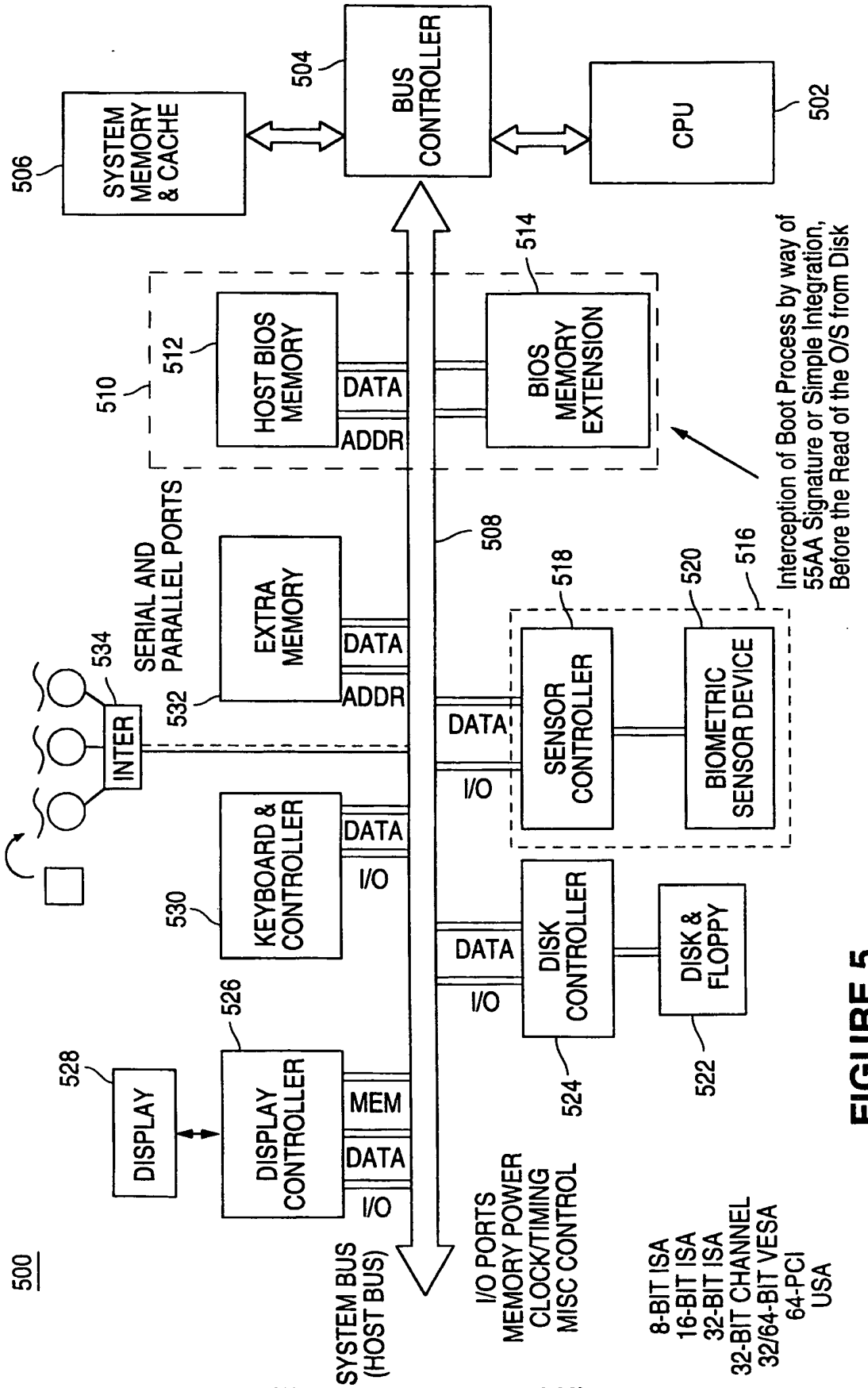

500
SYSTEM BUS (HOST BUS)
I/O PORTS
MEMORY POWER
CLOCK/TIMING
MISC CONTROL
8-BIT ISA
16-BIT ISA
32-BIT ISA
32-BIT CHANNEL
32/64-BIT VESA
64-PCI
USA
506
SYSTEM MEMORY & CACHE
504
BUS CONTROLLER
502
CPU
510
512
HOST BIOS MEMORY
DATA
ADDR
514
BIOS MEMORY EXTENSION
Interception of Boot Process by way of 55AA Signature or Simple Integration, Before the Read of the O/S from Disk
508
SERIAL AND PARALLEL PORTS
532
EXTRA MEMORY
DATA
ADDR
534
INTER
518
520
516
SENSOR CONTROLLER
BIOMETRIC SENSOR DEVICE
DATA
I/O
530
KEYBOARD & CONTROLLER
DATA
I/O
526
528
DISPLAY
DISPLAY CONTROLLER
MEM
DATA
I/O
DISK CONTROLLER
DISK & FLOPPY
DATA
I/O
524
522

FIGURE 5

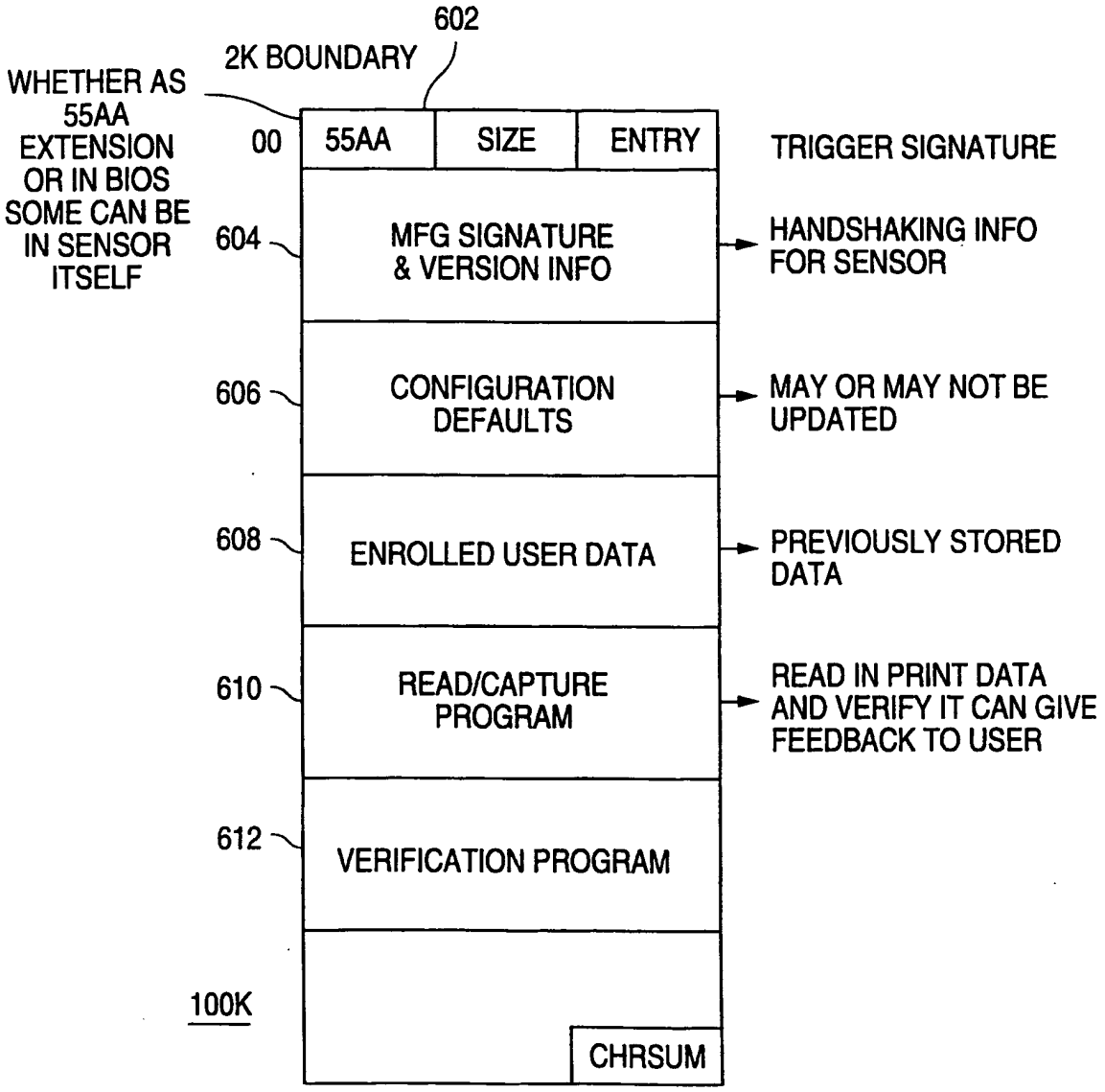

602
2K BOUNDARY
WHETHER AS 55AA EXTENSION OR IN BIOS SOME CAN BE IN SENSOR ITSELF
00
55AA
SIZE
ENTRY
TRIGGER SIGNATURE
604
MFG SIGNATURE & VERSION INFO
HANDSHAKING INFO FOR SENSOR
606
CONFIGURATION DEFAULTS
MAY OR MAY NOT BE UPDATED
608
ENROLLED USER DATA
PREVIOUSLY STORED DATA
610
READ/CAPTURE PROGRAM
READ IN PRINT DATA AND VERIFY IT CAN GIVE FEEDBACK TO USER
612
VERIFICATION PROGRAM
100K
CHRSUM

FIGURE 6

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/US 99/05218

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"BIOMETRIC ACCESS CONTROL IN A PERSONAL COMPUTER SYSTEM" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 41, no. 1, 1 January 1998 (1998-01-01), pages 753-756, XP000772281 ISSN: 0018-8689	1-12,14, 16-24, 26-29, 31-39, 41-53, 66-69, 71,72
Y	page 753, paragraph 1 - page 754, paragraph 5	55
A	page 754, paragraph 8 - page 755, paragraph 1	13,15, 25,30, 40,54, 56-65,70
	page 755, paragraph 4	
	page 755, paragraph 6 - page 756, paragraph 2	

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 July 1999	06/08/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/05218

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CA 2 156 236 A (BORZA STEPHEN J) 17 February 1997 (1997-02-17) page 2, line 26 - page 3, line 19; figures ---	1,16,28, 37,49, 66,71
Y	WO 93 17388 A (CLARK PAUL C) 2 September 1993 (1993-09-02) page 9, line 21 - page 11, line 14 ---	55
A	PATENT ABSTRACTS OF JAPAN vol. 095, no. 007, 31 August 1995 (1995-08-31) & JP 07 105142 A (CASIO COMPUT CO LTD), 21 April 1995 (1995-04-21) abstract -----	1,16,28, 37,49, 55,66,71

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte ional Application No
PCT/US 99/05218

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 2156236 A	17-02-1997	US 5867802 A	02-02-1999
WO 9317388 A	02-09-1993	AU 3777593 A	13-09-1993
		US 5448045 A	05-09-1995
JP 07105142 A	21-04-1995	NONE	